UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/518,583	03/03/2000	Chee-Seng Chow	047138/257085	5843

79901 7590 08/14/2008

Alston & Bird LLP
Bank of America Plaza
101 South Tryon Street
Suite 4000
Charlotte, NC 28280-4000

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
08/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CHEE-SENG CHOW, JAMES SUNG,
JEROME TSUNG-YAO CHEN and FIYAZ SUNDARJI

Appeal 2007-1256
Application 09/518,583
Technology Center 2100

Decided: August 14, 2008

Before JAMESON LEE, RICHARD TORCZON and SALLY C. MEDLEY, *Administrative Patent Judges*.

MEDLEY, *Administrative Patent Judge*.

DECISION ON APPEAL

A. Statement of the Case

GETHERE, Inc. ("GT"), the real party in interest, seeks review under 35 U.S.C. § 134(a) of a Final Rejection of claims 1-22, the only claims remaining in the application on appeal. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part.

The application on appeal was filed 03 March 2000.

The Examiner relies on the following prior art in rejecting the claims on appeal:

Anderson et al. ("Anderson")	6,144,959	Nov. 07, 2000
Win et al. ("Win")	6,453,353	Sept. 17, 2002

The Examiner rejected claims 1-4, 7-14 and 17-22 as anticipated under 35 U.S.C. § 102(e) by Win.

The Examiner rejected claims 5-6 and 15-16 as unpatentable under 35 U.S.C. § 103(a) as obvious over Win and Anderson.

B. Issues

The first issue is whether GT has sustained its burden of showing that the Examiner erred in rejecting appealed claims 1-4, 7-14 and 17-22 as anticipated under 35 U.S.C. § 102(e) by the prior art.

The second issue is whether GT has sustained its burden of showing that the Examiner erred in rejecting appealed claims 5-6 and 15-16 under 35 U.S.C. § 103(a) as obvious over the prior art.

C. Findings of Fact ("FF")

The record supports the following findings of fact as well as any other findings of fact set forth in this opinion by at least a preponderance of the evidence.

The Invention

1. The invention is related to a system and method for performing multiple user authentications with a single sign-on. Abs., Spec. 3, 5-7 and figs. 1 and 8-9.
2. Referring to figures 1 and 8-9 below [numbers from **figures 1**, **8** and **9** inserted], a user selects a remote server [**104**] and then performs a first user authentication [**802**], [**902**] with a user name and password within the user's Intranet [**120**]. Abs. Spec. 5-7 and 16-20 and figs 1 and 8-9.
3. An Intranet server can either determine if the user is a new user [**806**] or if the user wishes to create a new user profile or update an existing user profile [**904**]. Spec. 16-18 and figs 8-9.
4. The Intranet server forms an encrypted token [**808**-**818**], [**908**-**918**] that includes new user information [**806**] or new or updated profile information [**906**]. Spec. 16-19 and figs. 8-9.
5. The Intranet server transmits **[820**], [**920**] the encrypted token to the remote server [**104**]. Spec. 16-19 and figs. 8-9.
6. The remote server decrypts the token [**822**], [**922**], which has the effect within the remote server [**104**] of performing a second user authentication [**840**] [**940**] without the user needing to sign-on a second time. Abs., Spec. 16-19 and figs. 8-9.

GT's Figure 1 is reproduced below.

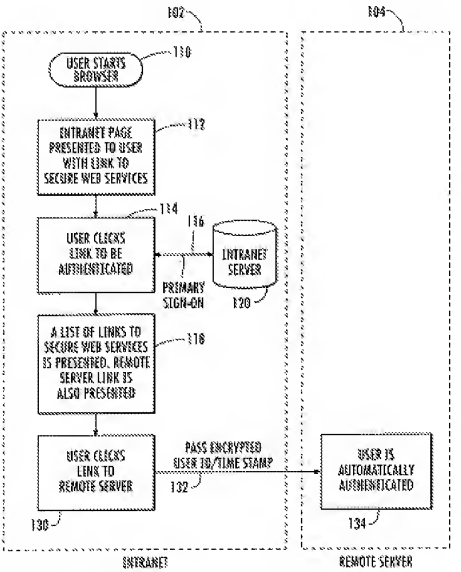

Figure 1 depicts user authentication via the user's Intranet and a Remote Server.

GT's Figure 8 is reproduced below.

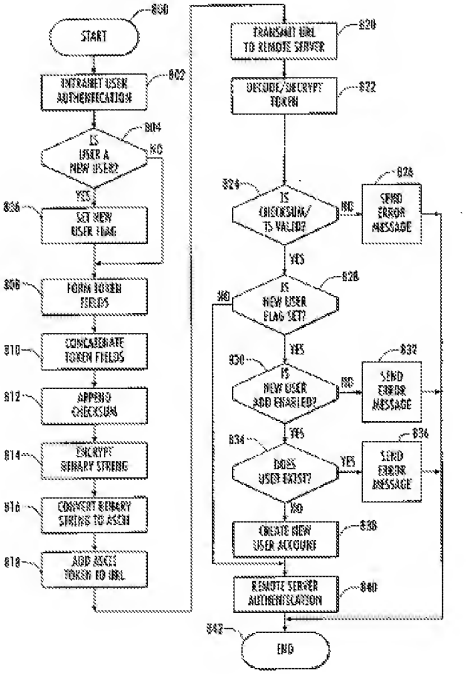

Figure 8 depicts the process of user authentication when a new user is determined.

GT's Figure 9 is reproduced below.

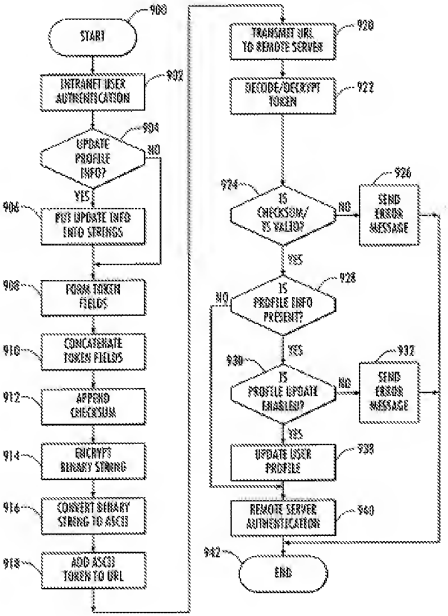

Figure 9 depicts the process of user authentication when a new user profile or update to an existing user profile is determined.

Claims on Appeal

7. GT's claims 1-22 are the subject of this appeal. App. Br.[1] 1.

8. Claims 1, 11, 21 and 22 are independent. App Br. 15-18.

9. Claims 2-10 and 12-20 are directly or indirectly dependent on claims 1 and 11 respectively. App Br. 15-18.

10. Claims 1-4, 7-14 and 17-22 stand or fall together. App. Br. 7-12.

11. Claims 5-6 and 15-16 stand or fall together. App. Br. 12-13.

[1] The Appeal Brief referred to hereinafter is the Substitute Appeal Brief filed 06 October 2006.

12. Representative claim 1 which we reproduce from the Claims Appendix of the Appeal Brief reads as follows:

> 1. A method of performing multiple user authentications with a single sign-on, comprising:
> performing a first user authentication;
> selecting a remote server subsequent to said first authentication;
> sending a token to said remote server containing authentication information responsive to said first authentication, wherein the token also contains information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user; and
> decoding said authentication information, wherein said decoding said authentication information induces a second user authentication.

Prior Art

Win

13. Referring to figure 1 below [numbers from **figure 1** inserted], Win describes a system [**2**] that enables users to log-in to the system once and thereafter access one or more resources during an authenticated session. Col. 5, l. 66-col. 6, l. 1.

14. Win also describes that users always access the same login page using browser [**100**] regardless of the number of resources 208 to which they need access thereby providing a mechanism of single secure log-in to Web resources. Col. 6, ll. 5-9; col. 9, ll. 45-50; and fig. 5A.

15. Win describes that a login page prompts a user for a name and password and the user enters the name and password into the login page using the browser [**100**]. Col. 9, ll. 42-44, 51-52; and fig. 5A.

16. Win describes that the browser [**100**] provides the name and password to the Access Server [**106**] and the user is considered authenticated if the name and password match information with the Registry Server [**108**]. Col. 6, ll. 42-44; col. 9, ll. 52-57; col. 22, ll. 47-48; and fig. 5A.
17. Win describes that after a user's login attempt is successful the system [**2**] presents the user with a Personalized Menu that assists the user in selecting a resource 208. Col. 6, ll. 10-15, 55-57.
18. Win describes that the user then selects and accesses the resource. Col. 6, ll. 15-16, 58-65.
19. Win describes that the resources 208 are stored on the Protected Server [**104**] and protected by a Runtime Module 206. Col. 6, ll. 59-61; and col. 7, ll. 34-36.
20. Win describes that after a user is authenticated, the Authentication Client module 414 of Access Server [**106**] calls the Authentication Client of Access Server [**106**] which requests profile information about the user from the Registry Server [**108**] that is coupled to the Access Server [**106**]. Col. 10, ll. 41-47; col. 6, ll. 21-23; and figs. 1, 5C.
21. Win describes that the Registry Server [**108**] returns the profile information to Access Server [**106**] and the Access Server Authorization Service creates a "user cookie" 528 and a "roles cookie" 530 containing encrypted data which are used to convey profile information to the browser [**100**]. Col. 10, ll. 48-53; col. 22, ll. 50-52; and figs 1, 5C.
22. Win describes that the profile information may comprise the user's name, locale information, IP address and information defining roles held by the user. Col. 10, ll. 49-51.

23. Win describes that the user cookie 528 contains a subset of the user profile information. Col. 10, ll. 53-54.
24. Win describes that the roles cookie 530 contains a list of the user's roles. Col. 10, l. 55.
25. Win describes that the cookies 528, 530 are passed from the Access Server [**106]** to the browser [**100]** which passes the cookies to every web server that it contacts in the same domain as the Access Server [**106]**. Col. 10, l. 67-col. 11, l. 2; and col. 22, ll. 56-59.
26. Win describes that when the user selects a resource 208, the browser [**100**] sends an open URL request and the cookie to a Protected Web Server [**104**] over an encrypted HTTP/SSL session. Col. 6, ll. 58-59; col. 22, ll. 63-64; and figs. 1-2.
27. The cookie is used by the resource to return information based on the user's name and roles. Col. 6, ll. 63-65; and col. 9, ll. 10-12.
28. Win describes that an administrator using the Administration Application [**114**] can create, delete and modify user, resource and role records. Col. 13, ll. 8-10, 17-19, 22-24; col. 18, l. 61-col. 19, l. 27; and fig. 10C.
29. Win describes that an Administration Application [**114**] is used to register and manage users, resources and roles by reading and writing information to and from a Registry Repository [**110**]. Col. 6, ll. 28-31; and col. 12, ll. 39-40.
30. Win describes that the Registry Server [**108**] is coupled to the Registry Repository [**110]** which stores information about users, resources and roles of the users. Col. 6, ll. 19-21.

31. Win describes that the Protected Web Server [**104**] is a web server with resources protected by the Runtime Module 206. Col. 6, ll. 60-61.

32. Win describes that if the Runtime Module 206 on the Protected Web Server [**104**] can decrypt the cookies successfully, it knows that the request comes from an authenticated user. Col. 6, ll. 61-63; col. 8, ll. 28-31; and col. 22, l. 65-col. 23, l. 2.

Figure 1 from Win is reproduced below.

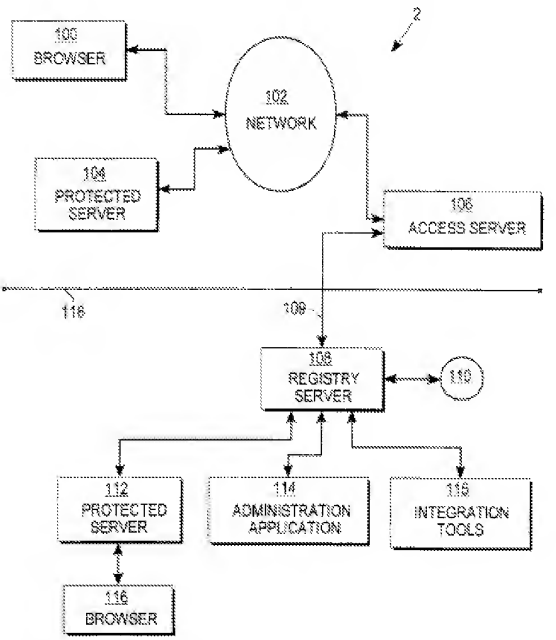

Figure 1 depicts the Registry Server, Registry Repository, Administration Application, Access Server, Browser and Protected Server.

Anderson

33. Anderson describes a Win32 Application Program Interface (API) including the NetUserAdd function to create a new user on a local Windows NT workstation. Col. 7, ll. 62-65.
34. Anderson describes that when the value of the parameter (to specify the domain, a user name, or a password) supplied by the program is null, the NetUserAdd function creates a user on the local workstation (i.e., client 102A) within the local access database 203. Col. 7, l. 65-col. 8, l. 7; and col. 8, ll. 1-3; and fig. 2A.
35. Anderson describes a directory services or NDS database 223 within a server 103A that includes a client workstation object 305G. Figs. 2A, 2C, 3A.
36. Anderson describes that login information 315 on the client workstation object 305G within the database 223 includes the dynamic log-in flag 317. Fig. 3B.
37. Anderson describes that the dynamic login flag 317 indicates whether user information should be retrieved from the client workstation object 305G within the database 223 of server 103A to create a user account on the client 102A. Col. 13, ll. 48-51.
38. Anderson describes a login process 207 that includes an authentication process 209 that is used to authenticate a user to the local client 102A as well as servers 103A and 103B. Col. 11, ll. 3-5; and fig. 2B.
39. Anderson describes that when dynamic login is enabled (flag is set) during the authentication process 209, 400 the client user name and workstation configuration information from workstation object 305G is

transferred to client 102A. Col. 13, ll. 59-62; col. 16, ll. 10-13, 22-30; and figs. 2B and 4-6.

40. Anderson describes that the authentication process 209 queries database 203 and verifies that the user name already exists. Col. 13, ll. 59-62; and Fig. 2B.

41. Anderson describes that if the user name exists, the authentication process 209 authenticates the user to the client 102A and access is granted to the user. Col. 13, ll. 62-65.

42. If the user name does not exist, the authentication process 209 creates a user account within the local access database 203. Col. 13, ll. 65-67.

Examiner's Findings

Win

43. The Examiner found that Win's description at column 6, lines 58-65 meets the claim limitations "sending a token to said remote server containing authentication information responsive to said first authentication, wherein the token also contains information regarding an account for the user including, at least one of a new account for the user and an update to an existing account for the user…". Final Rejection 3-4 and Ans. 3.

44. The Examiner found that Win's description at column 13, lines 22-53 meets the limitation "at least one of a new account for the user and an update to an existing account for the user". Ans. 3.

45. The Examiner found that the function "at least one of a new account for the user and an update to an existing account for the user" can be done at anytime or repeated at any desired time and therefore the cookies or token would be updated at this time. Ans. 3.

Win and Anderson

46. The Examiner found that Win does not describe the limitation "wherein the information regarding an account for the user in said token includes a new user flag". Final Rejection 5.

47. The Examiner found that Anderson describes the aforementioned limitation at column 7, line 62 through column 8, line 23. Final Rejection 3, 5 and Ans. 5-6.

48. The Examiner found that "a new user flag" is equivalent to "null parameter sent". Ans. 8.

GT's Arguments

Win

49. GT argues that Win does not disclose sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. App. Br. 8.

50. GT argues that Win does not describe updating of profile information with Remote Resources or a remote server. App. Br. 9, citing Win col. 9, ll. 33-35.

51. GT argues that in Win the updated information is not included with the cookies, since the updating occurs at the Access Server or Registry Server not the Protected Server. App. Br. 9 and Reply Br.[2] 3.

52. GT argues that Win also does not disclose that the cookies contain information regarding a new account for the user. App. Br. 9.

[2] The Reply Brief referred to hereinafter is the Reply Brief filed 23 February 2007.

53. GT argues that providing the capability to update or add a new account is not the same as providing information regarding a new account or an update to an account with a token to a remote server. App. Br. 9 and Reply Br. 3.
54. GT argues that Win only discloses that users may change their account profiles at the Access Server. App. Br. 9.
55. GT argues that unlike its invention, Win does not describe tokens or cookies reflective of new or updated account information are sent to a remote server or Protected Server. App. Br. 9.
56. GT argues that Win does not describe that the cookies contain information regarding an update to an existing account or information regarding a new account in addition to containing authentication information. App. Br. 9.
57. GT argues that independent claims 1, 11, 21 and 22 recite that the token contains authentication information regarding a new account and an update to an existing account for the user. Reply Br. 2.
58. GT argues that Win does not disclose the ability to modify user information contained on the cookie but instead disclose that the Authentication Client is capable of modifying a user's account information and roles that are stored on the Registry Repository. Reply Br. 2, citing Win col. 12, ll. 32-40.
59. GT argues that Win's cookies do not include information that may be modified, but Win describes that separate data files are stored at the Registry Repository and are capable of being modified. Reply Br. 3.
60. GT argues that Win's Authentication Client creates the cookies by requesting profile information at the Registry Server to create the user

cookie and role cookie that include a subset of user profile and role information. Reply Br. 3, citing Win col. 10, ll. 45-55.

61. GT argues that Win does not describe that the cookies contain authentication information regarding a new account and/or an update to an existing account for the user because the cookies created by the Authentication Client are based on stored information within the Registry Repository. Reply Br. 3.

62. GT argues that the cookies are only subsets of user information stored remotely at the Registry Server and Win does not teach or suggest that any new or updated user information is provided on the cookies. Reply Br. 3.

63. GT argues that the user and role cookies sent to the Protected Server only contain a subset of information stored at the Registry Server and were created in response to a login request at the Access Server. Reply Br. 3.

Win and Anderson

64. GT argues that neither Win or Anderson either alone or in combination, teach or suggest that the information regarding a user account for the user in the token includes a new user flag or that the remote server creates a new user account in response to the new user flag. App. Br. 12.

65. GT argues that Anderson describes that the dynamic log-in flag 317 is maintained in a directory services database 223 that is associated with a server 103A, which is transmitted to the client 102A during the log-in process. App. Br. 12, citing Anderson figs 2A and 3A.

66. GT further argues that Anderson describes that the log-in process 207 inspects the client workstation object 305G to determine whether a new user account should be created in the local access database 203 maintained in the client. App. Br. 12, citing Anderson col. 13, ll. 48-55.

67. GT argues that the dynamic log-in flag is not contained within a token that is sent from the client to the server, since Anderson describes the client workstation object, including the dynamic log-in flag, is sent from the server to the client to determine whether a new user account should be set up at the client. App. Br. 12-13, citing Anderson col. 13, ll. 48-55 and figs. 2A and 3A.

68. GT argues that Anderson's dynamic flag is not contained within a token that includes authentication information and information regarding a new account and/or update to an existing user account. App. Br. 13.

D. Principles of Law

"Anticipation under 35 U.S.C. § 102(e) requires that 'each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.'" *In re Robertson*, 169 F.3d. 743, 745 (Fed. Cir. 1999) (quoting *Verdegaal Bros., Inc. v. Union Oil Co.,* 814 F.2d 628, 631 (Fed. Cir. 1987)). Once the PTO has established a prima facie case of anticipation, the burden of production falls upon the applicant to establish entitlement to a patent. *In re Morris*, 127 F.3d. 1048, 1054 (Fed. Cir. 1997) (citations omitted).

"[T]he PTO gives a disputed claim term its broadest reasonable interpretation during patent prosecution." *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004). "Absent claim language carrying a narrow meaning, the PTO should only limit the claim based on the specification or prosecution

history when those sources expressly disclaim the broader definition." *Id.* at 1325.

E. Analysis

Rejection of claims 1-4, 7-14 and 17-22

Claims 1-4, 7-14 and 17-22 stand or fall together. FF[3] 10. We select independent claim 1 as the representative claim of this group. 37 C.F.R. § 41.37 (c)(1)(vii). Claim 1 recites the limitation "sending a token to said remote server containing authentication information responsive to said first authentication, wherein the token also contains information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user . . . ". FF 12.

The Examiner's position is that (1) Win describes sending a cookie (i.e., token) with encrypted information to a protected server (i.e., remote server) and (2) the cookie includes the user's names and roles and (3) an Administration Application can be used to enter information to establish the system and can be repeated at any desired time and therefore the cookie would be updated at this time. FFs 43-45.

GT presents a first position that Win does not disclose sending a token to a remote server that contains authentication information responsive to a first authentication *and* information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. FFs 49, 56.

We find that the claim 1 limitation of "sending a token to the remote server containing authentication information responsive to the first authentication" reads on Win's description of sending a cookie (i.e., a user

[3] FF denotes Finding of Fact.

cookie 528 and roles cookie 530) to the Protected Web Server [**104**] once the user is authenticated. FFs 20-23, 25-26. The resource 208 on the Protected Web Server uses the cookie to return information based on the user's name and roles. FF 27. In other words, the cookie sent to the Protected Web Server [**104**] includes authentication information because the cookie includes a user's name. We consider Win's user cookie 528 and roles cookie 530 collectively as also constituting a cookie because Win uses the singular general term "cookie" interchangeably with the two specific cookies together. FFs 21, 23-27, 32. Win also describes the user cookie 528 and roles cookie 530 are sent together to the browser [**100**] and Protected Server [**104**]. FF 25. As a result, we find that GT's token reads on the user cookie 528 and roles cookie 530 collectively as a singular "cookie". Furthermore, GT's Specification does not disclaim a broader interpretation of a "token".

We further find that the claim 1 limitation "wherein the token also contains information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user" reads on Win's description of a cookie comprising a user cookie 528 and a roles cookie 530 that is sent to the Protected Web Server [**104**]. FFs 20-22, 24-26. The resource on the Protected Web Server uses the cookie to return information based on the user's name and roles. FF 27. In other words, the cookie sent to the Protected Web Server includes information about the user's roles. Win further describes that role records can be created, deleted or modified by an administrator using Administration Application [**114**] and that this information is written to the Registry Repository [**110**] coupled to the Registry Server [**108**]. FFs 28-30. Win describes that Access Server [**106**], coupled to Registry Server [**108**], creates

the roles cookie 530 based on profile information retrieved from the Registry Server [**108**]/Registry Repository [**110**]. FFs 21-22, 24, 27, 30. The roles cookie 530 is then passed from the Access Server [**106**] to the browser [**100**] and to the Protected Web Server [**104**]. FFs 25-26. Thus, if an administrator has created, deleted or modified a user's roles and it has been written to the Registry Repository [**110**], the cookie comprising the roles cookie 530 that is created by the Access Server [**106**] from the profile information retrieved by the Registry Server [**108**]/Registry Repository [**110**] will reflect the created, deleted or modified user's roles. For these reasons, GT has not persuaded us that the Examiner erred in finding that claim 1 is anticipated by Win.

GT also presents the position that (1) Win does not describe updating profile information with Remote Resources or a remote server and (2) Win's created, modified or updated profile information is not included in the cookies that are sent to the Protected Server since the updating does not occur at the Protected Server but at the Access Server or Registry Server. FFs 50-55. The language of claim 1 does not require updating the user account information at a specific location. Since GT's arguments are directed to limitations not found in the claims, we are not persuaded by GT's arguments. As explained before, Win describes that created, deleted or modified user's roles are included in the roles cookie 530 that is ultimately sent to the Protected Server [**104**]. Therefore, we find GT's arguments that Win's cookies do not contain updated user profile information unpersuasive.

GT presents a third position that the claims require the token to include *authentication information regarding a new account and an updated account for the user* (emphasis added). FF 57. However, the language of claim 1only requires sending a token to a remote server with authentication

information and for the token to also have information regarding either a new or updated user account. Thus, we interpret the authentication information as distinct from the new or updated account information. As a result, we are not persuaded by GT's arguments since they are not commensurate with the scope of the claims.

GT presents a fourth position that the claims require the information contained on the tokens (i.e., cookies) to be modified. FFs 58-59. Representative claim 1 does not include language that requires the information on the tokens to be modified. Since GT is arguing limitations not found in the claims, we are not persuaded by GT's arguments.

Last, GT presents the position that Win provides no teaching or suggestion that any new or updated information is provided on the cookies because Win describes that the user and role cookies only include a subset of user profile and role information stored at the Registry Server or Registry Repository. FFs 60-63. We are unpersuaded by GT's arguments. As explained before, in Win, a user's roles can be created, modified or deleted and then stored in the Registry Repository [**110**] and subsequently retrieved by Access Server [**106**] which creates a roles cookie 530 that is ultimately sent to the resource 208 on Protected Server [**104**]. FFs 20-30. Win's cookie is used by the resource to return information based on the user's name and roles. FF 27. Thus, we know that the subset of information includes at least the user's role because the resource 208 had to have received the user's role in the cookie in order to use the user's roles to return information. If the user's roles have been created, modified or deleted, this user's roles information would be reflected in the cookie that is received by the resource 208 at Protected Server [**104**]. Therefore, GT has not persuaded

us that the Examiner erred in finding that Win's cookie contains updated information since Win describes the subset of user information in the user and roles cookie sent to the Protected Server contains new or updated information.

For all these reasons, we find that GT has not sustained its burden of showing that the Examiner erred in finding claims 1-4, 7-14 and 17-22 anticipated by Win.

Rejection of claims 5-6 and 15-16

Claims 5-6 and 15-16 are dependent on claims 1 and 11 respectively. FF 9. Claims 5 and 15 recite the further limitation "wherein the information regarding an account for the user in said token includes a new user flag". The Examiner found that Win does not disclose this limitation but that Anderson's description meets the claim limitation. FFs 46-47. In support of the rejection, the Examiner found that the new user flag is equivalent to "null parameter sent". FF 48.

GT argues that Anderson does not describe sending a token to a remote server that includes user information including a new user flag because Anderson describes a dynamic log-in flag 317 that is sent *from* a server 103A to a client 102A during a login process 207. FFs 64-68.

We agree with GT that Anderson describes that the dynamic log-in flag dynamic login flag 317 on the client workstation object 305 is sent from the server 103A instead of sent to the server 103A. FFs. 35-42. The Examiner also has not directed us to, and we can not find, where Anderson describes that the new user information within the local access database 203 created by the NetUserAdd function is sent to a server. FFs 33-34. Moreover, the Examiner has not directed us to, and we can not find, where Anderson

describes the "null parameter sent" that the Examiner found to be equivalent to "a new user flag".

As a result, GT has sustained its burden of showing that the Examiner erred in determining that claims 5-6 and 15-16 are obvious over the prior art.

F. Decision

Upon consideration of the appeal, and for the reasons given herein, it is

ORDERED that the decision of the Examiner rejecting claims 1-4, 7-14 and 17-22 as anticipated under 35 U.S.C. § 102(e) over Win is affirmed.

ORDERED that the decision of the Examiner rejecting claims 5-6 and 15-16 as unpatentable under 35 U.S.C. § 103(a) over Win and Anderson is reversed.

FURTHER ORDERED that no time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED IN-PART

MAT

Alston & Bird LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte NC 28280-4000